CLAIMS

1.   A method for masking digital data handled by an algorithm and factorized by a residue number system based on a finite base of numbers or polynomials prime to one another, comprising making the factorization base variable.

2.   The method of claim 1, wherein the factorization base is chosen from a look-up table of sets of numbers or polynomials prime to one another.

3.   The method of claim 2, wherein the set of numbers or polynomials prime to one another used for the factorization by residue number system is randomly selected from the look-up table, for each new application of the algorithm.

4.   The method of claim 1, wherein the factorization base is calculated by a pseudo-random generator.

5.   The method of claim 1, wherein the base is chosen to be compatible with the lengths of the numbers or polynomials processed by the algorithm.

6.   The method of claim 1, applied to input data already factorized by a residue number system in an original base, the input data undergoing a factorization base change and the result provided by the algorithm undergoing, preferably, an inverse transformation towards said original base.

7.   The method of claim 1, applied to input data not yet factorized.

8.   The method of claim 1, wherein one or several factorization base changes are performed during the execution of the algorithm.

9.   A circuit of algorithmic processing of data factorized by a residue number system based on a finite base of numbers or polynomials prime to one another, comprised of a circuit of selection or generation and of temporary storage of said base.

10.   The circuit of claim 9, comprising an element for storing a table of bases of numbers or polynomials prime to one another, said selection circuit selecting, at each application of the algorithm, a base from said table.

11.   The circuit of claim 9, comprising an element for checking the conformity between the base selected for application of the factorizations by residue number system and the calculation circuits of the circuit executing the algorithm.